Security threat mitigation trends in low-cost RFID systems

Joaquin Garcia Alfaro, Michel Barbeau, Evangelos Kranakis

Security Threat Mitigation Trends in Low-cost RFID Systems

Joaquin Garcia-Alfaro[1,2], Michel Barbeau[1], and Evangelos Kranakis[1]

[1] School of Computer Science,
Carleton University, K1S 5B6, Ottawa, Ontario, Canada.
{barbeau,kranakis}@scs.carleton.ca

[2] Open University of Catalonia,
Rambla de Poble Nou, 156, 08018, Barcelona, Spain.
joaquin.garcia-alfaro@acm.org

Abstract. The design and implementation of security threat mitigation mechanisms in RFID systems, specially in low-cost RFID tags, are gaining great attention in both industry and academia. One main focus of research interests is the authentication and privacy techniques to prevent attacks targeting the insecure wireless channel of these systems. Cryptography is a key tool to address these threats. Nevertheless, strong hardware constraints, such as production costs, power consumption, time of response, and regulations compliance, makes the use of traditional cryptography in these systems a very challenging problem. The use of low-overhead procedures becomes the main approach to solve these challenging problems where traditional cryptography cannot fit. Recent results and trends, with an emphasis on lightweight techniques for addressing critical threats against low-cost RFID systems, are surveyed.

Keywords: Radio Frequency Identification (RFID), Electronic Product Code (EPC), Wireless Security, IT Security, Security Threats, Privacy Threats.

1 Introduction

Radio Frequency Identification (RFID) is a wireless communication technology, based on analog and digital components, used to identify and track goods and people. Even though it has been used for more than seventy years (e.g., RFID was used in World War II for identifying enemy aircrafts), it is only now that this technology is re-emerging as an important communication paradigm that claims to revolutionize inventory and automation processes [61]. Examples are the use of RFID for supply chain inventory, health care management, animal identification, and anti-counterfeiting. However, while this technology is gaining importance with industrial suppliers, security and privacy concerns are raising, especially, among RFID consumers and end users.

An example is the introduction of low-cost RFID technology in the supply chain of the retail industry by means of the Electronic Product Code (EPC) concept. The EPC is a

unique code associated to a passive RFID tag that is placed on shipment pallets. The ability to identify and track these pallets, and their associated products, raise security and privacy concerns. These concerns become critical as retailers and manufacturers contemplate moving from pallet tagging to individual item tagging [61]. The possibility of rogue monitoring of people carrying these items is stimulating security and privacy research in both industry and academia. The insertion of cryptographic mechanisms in low-cost RFID tags is a promising solution to address the aforementioned concerns. However, current state-of-the-art solutions in cryptography must face significant challenges before being deployed in RFID technologies.

According to a research presented by Sarma in [62], the maximum cost of passive EPC tags should not exceed five cents to enable successful deployment on a world wide scale. This research also states that of these five cents, only one or two cents should be used for the manufacturing of the Integrated Circuit (IC). It is assumed that the available layout area for the implementation of the IC is in the range of 0.25mm^2 which, considering current CMOS technology, translate to a theoretical number of logic gates from two to four thousand. Not all the barriers investigated in [62] have been removed. The low-cost RFID technology of today is more expensive than what it was anticipated — around ten cents in large quantities. The inclusion of additional RFID features, especially for authentication and privacy purposes, may increase the total end-cost of tags up to fifteen cents or more per unit. Although Moore's Law predicts that digital devices fabricated on ICs will continue decreasing in price, cost of analogue devices (i.e., RF front-end of tags) will remain a constraint [12]. The inclusion of new elements must therefore be well planned.

Since the power used by low-cost RFID (passive) tags is derived from the signal received from readers, power restrictions also apply. The power consumption of a tag varies according to the nature of the operation being performed (e.g., responding to a query or writing data into the memory) and other parameters like the transmission rate, response time, and memory technology. Most of the operations performed in EPC tags require about five to ten microamps — although some special operations, such as writing operations, may require higher power. The power consumption of new security primitives must be within this range in order to allow low-cost tag production.

New security primitives must also work at the data rate of EPC applications. Current EPC applications demand an average reading speed of about two hundred tags per second. That leads to a data transmission rate requirement from tag to reader, of about 640 kbps; and a transmission rate from reader to tag of about 120 kbps. Delays associated to new security mechanisms (e.g., time to perform encryption or random number generation) may also affect the global performance. Delays must hence be taken into account and minimized. We can find in the literature several solutions that provide authentication and privacy mechanisms while meeting these challenging constraints. Most of the solutions can be classified in the following three categories: (1) lightweight cryptography based on the use of one-way hash-like primitives implemented in tags; (2) low-overhead and ultra-lightweight cryptography relying on the single use of on-tag pseudorandomness and simple arithmetic operations; and (3) alternative solutions avoiding the execution of cryptographic processes within tags. We survey, in the sequel,

recent contributions and trends according to these three categories. Our work aims at increasing the awareness of available security threat mitigation methods among RFID researchers and developers.

Paper organization. Section 2 surveys one-way hash-like solutions. Section 3 surveys proposals based on the single use of on-tag pseudorandomness and simple arithmetic operations. Section 4 surveys alternative approaches not requiring the necessity of on-tag cryptographic processes. Section 5 concludes the paper.

2 Lightweight Cryptographic Approaches

MAC (Message Authentication Code) based security protocols are among the first solutions discussed in the literature for securing low-cost RFID applications. In [65], for example, Takaragi et al. present a simple MAC-based approach that uses a static unrewritable 128-bit identifier stored, at manufacturing time, in every tag. The identifier is generated by the manufacturer using a unique secret key for each tag and a keyed hash function that accepts as input the secret key and a specific message. The secret key, hash function, and specific messages are communicated by the manufacturer to the client. Then, this information is shared among the clients' readers, to verify the integrity and authenticity of the exchanged messages. Therefore, this mechanism increases the technical difficulties of performing attacks against the integrity and authenticity of the messages. The main drawback is the use of static identifiers embedded in the tags at manufacturing time. Therefore, brute force attacks can break the secrets shared between readers and tags.

An enhanced solution relies on the use of hash-lock schemes for implementing access controls. In [69], Weis et al. propose a way to prevent unauthorized readers from reading tag contents. A secret is sent by authorized readers to tags using a trusted environment. Tags, equipped with an internal hash function, perform a hash on this secret and store it within their internal memory. Then, tags enter into a locked state in which they answer to any possible query with the computed hash. Weis et al. also describe proper ways of unlocking tags, if such an action is needed by authorized readers (i.e., to temporarily release private data). Regarding privacy threats, Ohkubo et al. propose in [49] the use of hash chains for the implementation of on-tag security mechanisms with evolving RFID identities. Avoine and Oechslin discuss in [2] some limitations of the approach. They propose an enhanced hash-based RFID protocol to address both authentication and privacy by using timestamps. Similarly, Henrici and Müller discuss in [25] some weaknesses in the hash-lock scheme presented in [69] and propose a new hash-based scheme intended to enhance privacy and authentication. Several other improvements and hash-based protocols, most of them inspired on lightweight cryptography research for devices with higher hardware capabilities such as smart cards, can be found in [48, 16, 43, 53].

2.1 Hardware Challenges and Limitations

Let us note that the aforementioned approaches require the implementation of one-way hash primitives within low-cost RFID tags. The requirement of reliable hash primitives implemented at the tag level is the main challenge associated with these proposals. Gate requirements of implementations based on standard one-way hash functions, such as MD4, MD5, and SHA-128/SHA-256, exceed the constraints pointed out in Section 1. The implementation of these functions require from seven thousand to over ten thousand logic gates; and from six hundred to over one thousand two hundred clock cycles [53]. The complexity of standard one-way hash functions is therefore an impediment for their deployment on low-cost RFID tags.

The use of standard encryption engines for the construction of hash operations has been discussed in the literature. For example, the use of Elliptic Curve Cryptosystems (ECC) [47] for the implementation of one-way hash primitives on RFID tags has been studied in [72]. Its use of small key sizes is seen as very promising for providing an adequate level of computational security at a relatively low cost [12]. An ECC implementation for low-cost RFID tags can be found in [4]. In [21], Feldhofer et al. present a 128-bit implementation of the Advanced Encryption Standard (AES) [14] on an IC of about three thousand five hundred gates with a power consumption of less than nine microamps at a frequency of 100 kHz. Although this implementation is considerably simpler than previous implementations of the AES algorithm, its requirements are still too high for low-cost RFID tags.

Alternative hash functions based on non-standard low-cost encryption engines is a third candidate. In [29], Israsena presents a hardware implementation of the Tiny Encryption Algorithm (TEA) [70] on an IC of about three thousand gates and with a consumption of about seven microamps. It fits the timing requirements of basic EPC setups where hundred of tags must simultaneously be accessed by the same reader. The implementation relies on very simple arithmetic and bitwise operators. The authors of TEA [70] claim that, despite its simplicity and ease of implementation, the complexity of the algorithm is equivalent to the one of DES (Data Encryption Standard) [47]. Variants of the TEA algorithm are, however, necessary for implementing hash functions. Mace et al. discuss in [46] some of the vulnerabilities of TEA, such as linear and differential cryptanalysis attacks, and present SEA (Scalable Encryption Algorithm). The strength of this proposal, due to its novelty, is not clear [12].

Other low-cost alternatives are the single use of Linear and Non Linear Feedback Shift Registers (LFSR & NLFSR). However, the simple use of LFSR & NLFSR as underlying mechanisms for the implementation of low-cost one-way hash functions — without further measures that add cost of extra hardware — lead to insecure implementations. For example, the use of the Cellular Automata (CA) model [71] for the implementation of one-way functions — typically built upon LFSR & NLFSR — has been proved to lead to insecure implementations [5, 12].

2.2 Physical One-Way Functions

The design of Physically Unclonable Functions (PUFs) and Physical Obfuscated Keys (POKs) is promising for the implementation of hash-like protocols on low-cost EPC tags. Half way between traditional cryptography and physical protection defenses, the ideas behind PUFs and POKs originated in [51] with the conception of optical mechanisms for the construction of Physical One-Way Functions (POWFs). Its use to securely store unique secret keys, in the form of fabrication variations, was proposed as a silicon prototype in [23]. The ideas were later improved in [45]. A coating PUF proposed in [64] claims an implementation that requires less than one thousand gates. The designs exploit the random variations in delays of wires and logic gates of an IC. For example, the silicon PUF presented in [23] receives input data, as a challenge, and launches a race condition within the IC: two transitions signals start propagating along different paths and are compared to determine which one comes first. To decide which signal comes first, a special controller produces a binary value.

The implementation of these proposals seems to have clear advantages at a cost of less than one thousand logic gates [64]. This technology provides a cost effective and reliable solution that successfully meet the constraints and requirements mentioned in Section 1. However, it also has several drawbacks. The difficulty of successfully modeling the circuits and their reliability is one of the obstacles that this technology must to face. The effects of environmental conditions and effects of the power supply voltage have also raised some concerns [12]. Some alternative proposals try to solve the drawbacks. Holcomb et al. propose in [26] an approach based on the CMOS SRAM memory of an electrical to generate physical fingerprints. The key idea is the usage of SRAM startup values as seeds of pseudorandomness. The authors claim that the use of 256 bytes of SRAM can yield 100 bits of true randomness each time the memory is powered up. While sound in theory, this technique is limited by memory space of current low-cost tags.

Challenge-response protocols are commonly used to implement security mechanisms in low-cost RFID tags using PUFs. An initial approach presented in [58], and based on PUFs proposed in [23], consists of a challenge-response scheme that probabilistically ensures unique identification of RFID tags. The back-end system of this approach must learn challenge-response pairs for each PUF/tag. It then uses these challenges (hundreds of them) at a time, to identify and authenticate tags. Unique identification of tags is probabilistic. The exposition of tag identifiers to eavesdroppers, and lack of state and randomness in tag responses, make the approach vulnerable to tracking and location threats. Moreover, the great number of challenges that are necessary between readers and tags for the completion of the identification process increases tag response delay and power consumption.

An alternative protocol is presented in [67]. Tuyls and Batina discuss an off-line PUF-based mechanism for verifying the authenticity of tags using the PUF technology presented in [64]. Similarly to the traditional approaches presented in [31, 36], where readers and tags define ad hoc secrets, the PUF-based approach uses instead the physical structure embedded within tags to generate unique keys. A key extraction algorithm

from noisy (binary) data is presented in [67]. The usage of PUF-based keys simplifies the process of verifying tag authenticity. The combination of unique keys generated on-board together with public key cryptography techniques (e.g., use of signatures) avoid leaking the static single identifier and hence increase the technical difficulties for an attacker to carry on location tracking threats. The main drawback of the approach is the need of large storage space and reliable searching processes on back-end servers in order to link readers with PUF/tag identifiers. The use of public key and digital signatures, based on Elliptic Curve Cryptography (ECC), is another important constraint of the approach.

Bolotnyy and Robins propose in [6] a complete set of adapted MAC protocols based on PUFs aiming to simplify the challenge-response communication scheme of previous proposals, and the requirement of traditional cryptographic primitives. Each tag generates multiple identifiers based on embedded PUFs. The approach only addresses static identification and is vulnerable to location tracking attacks. The approach does not solve the necessity of huge lists of challenge-response pairs for each PUF/tag which must be stored on back-servers connected to the readers. Indeed, once a given pair is sent, it must not be used anymore. Otherwise, the protocol cannot guarantee that an adversary eavesdropping data will not gain advantage by performing a replay attack.

3 Low-overhead and Ultra-lightweight Solutions

The use of on-tag Pseudo Random Numbers Generators (PRNGs) to enhance the security and privacy of RFID systems is another candidate. In fact, most of the approaches, if not all, presented in Section 2 require the use of PRNGs to guarantee correctness. For example, the enhanced hash-lock scheme presented by Weis et al. in [69] relies on the use of on-tag PRNGs and efficient pseudorandomness for mitigating privacy threats like location tracking. Another example is the need of combining PRNGs and hash chains to enable the proposal of Ohkubo et al. presented in [49]. More recently, a protocol presented in [66], called YA-TRAP, reduces the need of hash-based protocols by combining pre-computed hash-tables for tag verification processes with timestamps and generation of pseudorandom numbers. Similar requirements apply on all the other protocols surveyed in Section 2 — in order to address location tracking problems. From a hardware point-of-view, the insertion of robust one-way hash functions and PRNGs in the constrained environment of low-cost RFID tags makes the implementation of those proposals very challenging and, unrealistic for real world applications.

The use of pseudorandomness for increasing low-cost RFID security is often questioned because robust designs are complex to implement on low-cost RFID devices. The complexity of the implementation of robust PRNGs is equivalent to the complexity of the implementation of robust one-way hash-functions and/or equivalent encryption engines [47]. However, since the ratification of the EPCglobal standard EPC Class-1 Generation-2 (Gen2 for short) [20] and ISO standards ISO/IEC 18000-6C [28] for the usage of on-tag PRNGs on low-cost RFID devices, the number of single PRNG-based solutions has increased in the industry and academia research. The existence of PRNG

hardware already deployed on most of the low-cost RFID tags justifies the convenience of this second category of security threat mitigation mechanisms.

Juels and Weis present in [36] an unidirectional authentication protocol based on the secure human identification protocol series proposed by Hopper and Blum [27]. The new protocol, called by the authors HB+, aims at preventing active attacks against the authenticity of low-cost RFID systems. The resistance of HB+ against active adversaries is proved by the authors using an statistical conjecture [13] to bound the difficulty of learning a secret (e.g., ID of the tag) given a sequence of randomly chosen vectors with embedded noisy information. The authors claim that the protocol can be implemented on low-cost tags since it only requires PRNG primitives in tags and implementation of very simple operations, such as bitwise-and and xor. Some security issues of the HB+ protocol were reported in [39, 57]. They propose enhancements to address active attacks. However, neither the original HB+ protocol nor its sequels consider authentication of the readers and location tracking attacks. Regarding these issues, we can find in [38] a new low-overhead protocol by Karthikeyan and Nesterenko for mutual authentication of tags and readers. The requirements of this protocol are modular algebra operations, such as multiplication of matrices, and on-tag PRNG primitives. Based on similar requirements, such as on-tag PRNG and matrix algebra operations, Dolev et al. present in [17] two low-overhead proactive unidirectional protocols, called PISP (Proactive Informational Secure Protocol) and PCSP (Proactive Computationally Secure Protocol), with evolving on-tag secrets that expands indefinitely over time. Both PISP and PCSP are compared and contrasted in a joint publication appeared in [19]. The security of these protocols relies on the difficulty of recovering the operands used on both sides (tags and readers) to synchronize shared secrets. Memory space on current low-cost tags is another limitation to the security of these approaches. An enhanced version of the PCSP protocol, presented in [18], aims at preventing active attacks against the protocol while keeping similar requirements, i.e., on-tag PRNG primitives and matrix operations.

Burmester, Le, and de Medeiros proposed in [7] a new low-overhead protocol, called O-TRAP (Optimistic Trivial RFID Authentication Protocol). Like other protocols surveyed in this section, O-TRAP relies on the use of PRNG primitives in tags and some other simple bitwise operations. O-TRAP is specially designed to prevent privacy attacks while guaranteeing anonymous authentication. The protocol behaves in a manner similar to the hash-lock approach introduced in Section 2. Common secret, shared between readers and tags, are proposed in their scheme to update pseudonyms stored within tags. Like in the hash-lock approach introduced by Weis et al. in [69], readers must access back-end databases to map pseudonyms to true identities. The security of the protocol is proved using the universal composability (UC) model [8]. It is shown that the O-TRAP protocol meets the UC definition of anonymous authentication and anonymous key exchange. However, the O-TRAP protocol fails to satisfy the stronger privacy definitions, such the one stated by Juels and Weis in [37] establishing that privacy countermeasures must guarantee both anonymity and untraceability. Juels and Weis point out the possibility of attacking the O-TRAP protocol by de-synchronizing tags. This allow

active attacker to uniquely identify them and carry on location tracking attacks. An attack against the untraceability of the O-TRAP protocol is presented in [50].

Similar attacks exploit existing vulnerabilities in the state-of-the-art of the ultra-lightweight series of authentication protocols. Ultra-lightweight authentication protocols, such as [54–56, 11], try to eliminate the necessity of hash and PRNG primitives, and involve only simple bitwise and modular arithmetic on-tag operations. The computation of costly operations, such as the generation of pseudorandom numbers, is done at the reader side. Although this fact benefits the implementation of such countermeasures on the constrained environment of low-cost RFID tags, none of these proposals seems to be resistant to either active or passive attacks. The set of authentication techniques presented by Peris-Lopez et al. in [54–56] were reported to be vulnerable by Li and Wang, and Li and Deng to, respectively, the de-synchronization attacks and full-disclosure attacks. Improvements of these techniques, presented by Chien in a new protocol called SASI [11] have recently been reported as vulnerable by Cao, Bertino, and Lei in [9]. These recent cases show how challenging it is to design adequate procedures given the low-cost requirement of the RFID paradigm.

4 Avoidance of On-tag Cryptographic Processes

Several results, such as [32, 40, 30, 31], are not relying on the execution of cryptographic algorithms in tags. One of the earliest proposals is the re-encryption scheme of Juels and Pappu presented in [32]. It provides privacy and security for banknotes embedding RFID tags. The approach uses public key cryptography and digital signatures. The operations are, although, performed outside the tags. The scheme consists of a public-key cryptosystem and two authorities: a central bank and a law enforcement agency. Both authorities hold an independent pair of public and private keys associated to each banknote. The central bank authority assigns a unique serial number to each banknote. To do so, the bank uses its private key to sign the unique serial number. The signature and the serial number of the banknote are printed on the banknote as optical data. Then, by using the public key of the law enforcement agency, the bank encrypts the digital signature, unique serial number, and a random number. The resulting ciphertext is stored into a memory cell of the RFID tag. This memory cell is keyed-protected. The tag only grants write access to this memory cell if it receives an access key derived from the optical data. The random number used to create the ciphetext is also stored into a separated memory cell of the tag. This second memory cell is also keyed-protected. The tag only grants read or write access to this memory cell if it receives an access key derived from the optical data.

By using this previous approach, banknote bearers must verify first the digital signature, printed in the banknote as optical data, using the public key of the central bank. Second, they must also verify the validity of the ciphertext stored in the RFID tag. To do so, the bearer encrypts the digital signature, serial number, and random number stored in the memory of the tag, using the public key of the law enforcement agency and the optical data. If one of these two verification processes fails, the authorities must be warned. To

avoid using the same ciphertext on every interaction, the authors propose the use of a re-encryption process that can be performed by banknote bearers without the necessity of accessing the private keys of the law enforcement authority. Based on the algebraic properties of the El Gamal cryptosystem [47], the initial ciphertext is transformed into a new unlinkable ciphertext, using the public key of the law enforcement authority [32]. This re-encryption process is performed outside the tags. Although the whole process is too complex for use in low-cost RFID scenarios, it is one of the first solutions that appeared in the literature for deploying cryptographic protocols in RFID applications without the need to embed cryptographic primitives in tags.

The work presented by Kinosita et al. in [40] consists of an anonymous ID scheme, in which a tag contains only a pseudonym that is periodically rewritten. Similarly, the approach of Juels in the work *Minimalist Cryptography for Low-Cost RFID Tags* [30] suggests a very light-weight protocol for mutual authentication between tags and readers based on one-time authenticators. Both solutions rely on the use of pseudonyms and keys stored within tags and back-end servers. Pseudonyms are used instead of real identifiers (e.g., instead of the EPC codes in supply chain RFID applications). Each tag contains a small collection of pseudonyms, according to the available memory. A throttling process, is used to rotate these pseudonyms. Each time a tag is interrogated by a reader, a different pseudonym selected at random is returned. Authorized readers have access to the complete list of pseudonyms of each tag and can correlate the identity of the responses they receive. Without the knowledge of this list, unauthorized readers are unable to infer any information about the numerous occurrences of the same tag. The process also forces tags to slow their transmissions when queries come too quickly, as a defense to brute-force attacks. The memory space in current low-cost tags is the main limitation of this approach. Although enhancements can be used to update the list of pseudonyms, communication costs and integrity threats still remain as main drawbacks. A similar, though lighter-weight, protocol for mutual authentication between readers and tags is presented by Juels in [31]. This time, the Personal Identification Number (PIN), associated to the kill command of EPC Gen2 tags [20], is used to implement the protocol. The main idea is that even if the EPC data of a tag is skimmed, the PIN remains secret. This way, cloned tags can be detected by testing, without killing the tag, if the kill password matches the original one stored in a back-end database. The risk of exposing the kill PIN of a given tag is however an important drawback of this approach.

Many signal-, power-, and blocking-based defenses, such as shielding of tags, use of noise, and third party guardians, can be found in the literature. The use of distance measurements to detect rogue readers has been discussed in [22]. Fishkin et al. propose the inclusion of low-cost circuitry in tags to use the signal-to-noise ratio of readers as a metric for trust. In [24], a similar assumption is used to determine if a reader is authorized to read the tag contents according to its physical distance. Castelluccia and Avoine propose in [10] the use of additional tags with better hardware capabilities than low-cost RFID hardware capabilities, to generate noise on the communication channel between readers and low-cost tags. The objective is to thwart possible eavesdroppers. Similar software-based blocking strategies can be found in [34, 60]. Third party compo-

nents with cryptographic features to perform authentication and acting as intermediaries between readers and tags have been proposed in [59, 35]. The management of these components in real world scenarios like the supply chain of the retail industry is a problem and the main drawback of these proposals. Finally, the use of radio fingerprinting to detect characteristic properties of transmitted signals has also been considered in the literature. Cole and Ranasinghe [12] consider, however, that this technique is difficult to develop in RFID applications and that the benefits of using it, regarding performance, price and required implementation surface in tags, are unclear. Avoine and Oechslin discuss in [1] the prevention of traceability attacks via radio fingerprinting. They also conclude that obtaining radio fingerprints of tag is very expensive and difficult. The myriad of tags in circulation in future RFID scenarios would make impracticable the distinction of tags.

4.1 Towards Secret-Sharing Strategies

As an evolution of the minimalist cryptography approach presented by Juels in [30], and using lists of pseudonyms, the use of secret-sharing schemes is proposed by Langheinrich and Martin in [41, 42] for solving authentication and privacy threats in low-cost RFID scenarios (e.g., supply chain applications of the retail industry). The work presented in [41] simplifies the lookup process performed from readers to back-end databases for identifying tags, while guaranteeing authentication and tracking resistance. Tag identifiers, seen in this work as the secrets, are encoded as a set of shares and stored in the internal memory of tags. The mechanism used by the authors to encode the shares is based on the *(t-n)*-threshold schemes of Shamir [63]. When the shares are cryptographically combined at the reader side, original tag identifiers are reconstructed. To prevent brute-force scanning from unauthorized readers — trying to obtain the complete set of shares — the authors propose a time-limited access that controls the amount of data sent from tags to readers. At the same time, a cache based process ensures that authorized readers quickly identify tags. Langheinrich and Martin extended the previous proposal to spread the set of shares across multiple tags [42]. Still based on the Shamir's secret sharing schemes, this approach encodes the indentifier of an item tagged with multiple RFID devices by distributing it into multiple shares stored within its tags. Authentication and privacy are enforced by requiring readers to obtain and combine the set of shares.

In [33], Juels, Pappu, and Parno present another secret-sharing based approach, but based on a dispersion of secrets strategy rather than an aggregation strategy — as used by Langheinrich and Marti in [41, 42]. Two different schemes are discussed: dispersion of secrets across space and dispersion of secrets across time. In both schemes, a secret that is used to encrypt RFID identifiers (e.g., the EPC codes) is split in multiple shares and distributed among multiple parties. The construction and recombination of shares are based on the use of error-correcting codes. In order to identify a tag, a party must collect a number of shares. Privacy is achieved by the dispersion of secrets and encrypted identifiers. The dispersion approach helps to improve the authentication process between readers and tags, as tags move through a supply chain. Assuming that a

given number of shares is necessary for a reader to obtain the EPC codes assigned to a pallet, for example, a situation where the number of shares obtained by a reader is not sufficient to reach the threshold leads to conclude that unauthorized tags are present on the pallet. The approaches presented in [33] increase the resistance of tags against unauthorized scanning by dispersing tag populations outside the supply chain. Without the space proximity to other tags with equivalent shares, an unauthorized reader cannot obtain the sufficient number of shares required to recover the original identifier of tags and items. A clear advantage of this approach is that it can be implemented on low-cost RFID tags, such as EPC Gen2 [20] tags, without requiring changes to the current specifications. Only an upgrade of readers is necessary. No real-world tests of the proposals have been conducted. The authors claim, although, that experiments for pharmaceutical products in a closed-loop supply chain are going to be conducted in the future. The main drawback of this approach is the amount of tag memory space required for storing the shares. A shrinking of key shares must be performed a priori in order to apply the scheme on current EPC tags. Other problems, such as tracking and information leaks due to the interaction between authorized readers and tags, must also be solved before deploying the schemes.

5 Conclusions

The constrained environment and threat model associated to low-cost RFID tags have stimulated the creation of a vast number of proposals to provide low-overhead security threat mitigation mechanisms in these devices. Vulnerable designs appeared in recent literature, such as the lightweight authentication protocols presented by Vajda and Buttyán in [68] (whose vulnerabilities were recently reported by Defend, Fu, and Juels in [15]), the set of ultra-lightweight authentication techniques presented by Peris-Lopez et al. in [54–56] (which were reported as vulnerable to passive [3] and active [44] attacks), and enhancements of these proposals, like the SASI protocol [11] (recently reported by Cao, Bertino, and Lei in [9] as vulnerable), show how challenging it is to design adequate procedures given the constraints. We surveyed lightweight defenses that can be useful to reduce the risk of threats. We addressed the methods according to three different perspectives: (1) one way hash-like defenses, (2) solutions relying on the single use of on-tag pseudorandomness and simple arithmetic operations; and (3) mechanisms not requiring the execution of cryptographic processes in the tags.

Regarding the first perspective, we pointed out the hardware challenges which to the best of our knowledge, are important obstacles for deployment in real world low-cost RFID scenarios like the supply chain of the retail industry. Physical One-Way Functions (POWFs) and Physically Unclonable Functions (PUFs) are a promising evolution of traditional hash-based protocols, but at a feasible production cost. Their sensitivity to physical noise, the large number of challenges and training session between readers and tags to guarantee adequate identification, and the difficulty to model and analyze, are open lines of research. In the second perspective, we pointed out the memory space and de-synchronization flaws as main limitations. The evolution of these solutions toward

strategies that avoid the execution of on-tag cryptographic processes is heading recent researches. We pointed out the use of secret sharing strategies as a promising foundation for the management of keys for the design of authentication protocols and for dealing with privacy issues. Main drawbacks are the management of information leaks due to the interaction between readers and tags, and tracking of tags.

Acknowledgments — The authors graciously acknowledge the financial support received from the following organizations: Natural Sciences and Engineering Research Council of Canada (NSERC), Mathematics of Information Technology and Complex Systems (MITACS), Spanish Ministry of Science and Education (TSI2007-65406-C03-03 "E-AEGIS" and CONSOLIDER CSD2007-00004 "ARES" grants), and *La Caixa* (Canada awards).

References

1. G. Avoine and P. Oechslin. RFID Traceability: A multilayer problem. In Andrew Patrick and Moti Yung, editors, *Financial Cryptography – FC'05*, LNCS, 3570, pages 125–140, The Commonwealth Of Dominica, February–March 2005. IFCA, Springer.
2. ——. A scalable and provably secure hash based RFID protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114, 2005.
3. M. Barasz, B. Boros, P. Ligeti, K. Loja, and D. Nagy. Breaking LMAP. In *Conference on RFID Security*, Malaga, Spain, July 2007.
4. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for RFID-tags. Cryptology ePrint Archive, Report 2006/227, 2006.
5. S. R. Blackburn, S. Murphy, and K. G. Paterson. Comments on 'theory and applications of cellular automata in cryptography'. *IEEE Trans. Softw. Eng.*, 23(9):637–638, 1997.
6. L. Bolotnyy and G. Robins. Physically unclonable function-based security and privacy in RFID systems. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 211–220, New York, USA, March 2007. IEEE Press.
7. M. Burmester, T. Van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication. In *2nd International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)*. 2006. IEEE Press.
8. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *IEEE Symp. On Foundations of Computer Science (FOCS 2001)*, pages 136–145, 2001.
9. T. Cao, E. Bertino, and H. Lei. Security Analysis of the SASI Protocol. *IEEE Transactions on Dependable and Secure Computing*, May 2008. preprint, http://doi.ieeecomputersociety.org/10.1109/TDSC.2008.32.
10. C. Castelluccia and G. Avoine. Noisy tags: a pretty good key exchange protocol for RFID tags. In: *International Conference on Smart Card Research and Advanced Applications (CARDIS'06)*, Spain, April 2006. Springer.
11. H. Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, December 2007.
12. P. Cole and D. Ranasinghe, editors. *Networked RFID Systems and Lightweight Cryptography — Raising Barriers to Product Counterfeiting*. Springer, 1rst edition, 2008.
13. J. M. Crawford, M. J. Kearns, and R. E. Shapire. The Minimal Disagreement Parity Problem as a Hard Satisfiability Problem. Tech. rep., Computational Intelligence Research Laboratory and AT&T Bell Labs, February 1994.

14. J. Daemen and V. Rijmen. *The Design of Rijndael: AES–the Advanced Encryption Standard*. 2002. Springer.
15. B. Defend, K. Fu, and A. Juels. Cryptanalysis of two lightweight RFID authentication schemes. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 211–216, New York, USA, March 2007. IEEE Press.
16. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece, September 2005. IEEE Press.
17. S. Dolev and M. Kopeetsky. Secure communication for RFIDs proactive information security within computational security. In *8th Int'l Symposium on Stabilization, Safety, and Security of Distributed Systems*, LNCS, 4280, pages 290–303. 2006. Springer.
18. S. Dolev, M. Kopeetsky, and Adi Shamir. RFID Authentication Efficient Proactive Information Security within Computational Security. Tech. rep., Department of Computer Science, Ben-Gurion University, July 2007.
19. S. Dolev, M. Kopeetsky, T. Clouser, and M. Nesterenko. Low Overhead RFID Security. In chapter 32 of S. A. Ahson and M. Ilyas, editors, *RFID Handbook: Applications, Technology, Security, and Privacy*, pages 589–602, CRC Press, 2008.
20. EPCglobal. EPC Radio-frequency identity protocols Class-1 Generation-2. Technical report, http://www.epcglobalinc.org/standards/, January 2005.
21. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer.
22. K. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. In *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS 2004*, LNCS, 3313, pages 42–53, Heidelberg, Germany, August 2005. Springer.
23. B. Gassend, D. Clarke, M. Dijk, and S. Devadas. Silicon physical random functions. In *9th ACM conference on Computer and communications security*, pages 148–160, New York, NY, USA, 2002. ACM.
24. G. Hancke. Noisy carrier modulation for HF RFID. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
25. D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.
26. D. Holcomb, W. Burleson, and K. Fu. Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags. In *Third International Conference on RFID Security - RFIDSec 2007*, Malaga, Spain, 2007.
27. N. Hopper and M. Blum. Secure human identification protocols. In *Advances in Cryptology-ASIACRYPT*, LNCS, 2248, pages 52–66. 2001. Springer.
28. ISO/IEC 18000-6:2004/amd:2006. Technical report, http://www.iso.org/, 2006.
29. P. Israsena. Securing ubiquitous and low-cost RFID using tiny encryption algorithm. In *Intn0l Symp. on Wireless Pervasive Computing*, Thailand, January 2006. IEEE Press.
30. A. Juels. Minimalist cryptography for low-cost RFID tags. In *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164, Amalfi, Italia, September 2004. Springer.
31. ——. Strengthening EPC tags Against Cloning. In *WiSe '05: Proceedings of the 4th ACM workshop on Wireless security*, pages 67–76, New York, NY, USA, 2005. ACM Press.
32. A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In *Financial Cryptography – FC'03*, LNCS, 2742, pages 103–121, Guadeloupe, French West Indies, January 2003. Springer.

33. A. Juels, R. Pappu, and B. Parno. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. In *USENIX Security Symposium*, San Jose, CA, July-August 2008. USENIX.
34. A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *8th ACM Conf. Comput. Commun. Security*, pages 103–111, 2003.
35. A. Juels, P. Syverson, and D. Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. In: *5th Workshop on Privacy Enhancing Technologies*, 2005. Springer.
36. A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In *Advances in Cryptology – CRYPTO'05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308, USA, 2005. IACR, Springer.
37. ——. Defining Strong Privacy for RFID. In *5th Annual IEEE International Conference on Pervasive Computing and Communications*, pages 342–347, 2007. IEEE Press.
38. S. Karthikeyan and M. Nesterenko. RFID security without extensive cryptography. In *3rd ACM workshop on Security of ad hoc and sensor networks*, pages 63–67, USA, 2005.
39. J. Katz and J. Shin. Parallel and concurrent security of the HB and HB$^+$ protocols. In *Advances in Cryptology – EUROCRYPT'06*, LNCS, Russia, 2006. Springer.
40. S. Kinosita, F. Hoshino, T. Komuro, A. Fujimura, and M. Ohkubo. Non-identifiable anonymous-ID scheme for RFID privacy protection, 2003. *http://www.autoidlabs.com/whitepapers/KEI-AUTOID-WH004.pdf*.
41. M. Langheinrich and R. Marti. Practical Minimalist Cryptography for RFID Privacy. *IEEE Systems Journal*, 1(2):115–128, December 2007.
42. ——. RFID privacy using spatially distributed shared secrets. In *4th International Symposium of Ubiquitous Computing Systems*, LNCS, 4836, pages 1–16, 2007. Springer.
43. S. Lee, T. Asano, and K. Kim. RFID mutual authentication scheme based on synchronized secret information. In *Symposium on Cryptography and Information Security*, 2006.
44. T. Li and R. Deng. Vulnerability analysis of EMAP - an efficient RFID mutual authentication protocol. In *Second International Conference on Availability, Reliability and Security – AReS 2007*, Vienna, Austria, April 2007.
45. D. Lim, J Lee, B. Gassend, G Suh, M. Dijk, and S. Devadas. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(10):1200–1205, 2005.
46. F. Mace, F. Standaert, and J. Quisquater. ASIC implementations of the block cipher sea for constrained applications. In *Conference on RFID Security*, pages 103–114, Spain, 2007.
47. A. J. Menezes, P.C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.
48. D. Molnar and D. Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In *Conference on Computer and Communications Security – ACM CCS*, pages 210–219, Washington, DC, USA, October 2004. ACM Press.
49. M. Ohkubo, K. Suzuki, and S. Kinoshita. Efficient hash-chain based RFID privacy protection scheme. In *International Conference on Ubiquitous Computing – Ubicomp, Workshop Privacy: Current Status and Future Directions*, Nottingham, England, September 2004.
50. K. Ouafi and R. Phan. Privacy of Recent RFID Authentication Protocols. In *4th International Conference Information Security Practice and Experience (ISPEC 2008)*, volume 4991 of *Lecture Notes in Computer Science*, pages 263–277, 2008. Springer.
51. R. Pappu. *Physical One-Way Functions*. PhD thesis, MIT, 2001.
52. P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. LAMED, A PRNG for EPC Class-1 Generation-2 RFID specification. *Computer Standards & Interfaces*, 2008. Elsevier.
53. ——. An efficient authentication protocol for RFID systems resistant to active attacks. In *Emerging Directions in Embedded and Ubiquitous Computing*, volume 4809 of *Lecture Notes in Computer Science*, pages 781–794. Springer, 2007.

54. ——. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. Ecrypt, July 2006. Austria.
55. ——. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *International Conference on Ubiquitous Intelligence and Computing – UIC'06*, volume 4159 of *Lecture Notes in Computer Science*, pages 912–923. Springer-Verlag, September 2006.
56. ——. EMAP: An efficient mutual authentication protocol for low-cost RFID tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361. Springer-Verlag, November 2006.
57. S. Piramuthu. HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In *Collaborative Electronic Commerce Technology and Research – CollECTeR 2006*, Basel, Switzerland, June 2006.
58. D. Ranasinghe, D. Engels, and P. Cole. Low-cost RFID systems: Confronting security and privacy. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.
59. M. Rieback, B. Crispo, and A. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In *Australasian Conference on Information Security and Privacy –ACISP 2005*, LNCS, 3574, pages 184–194, 2005. Springer.
60. ——. Keep on blockin'in the free world: Personal access control for low-cost RFID tags. In 13th Cambridge Workshop on Security Protocols, 2005. Springer.
61. G. Roussos. Enabling RFID in retail. *IEEE Computer*, 39(3):25–30, March 2006.
62. S. Sarma. Toward the 5 cent tag. White Paper, November 2001. Auto-ID Center.
63. A. Shamir. How to share a secret. In Commun. of the ACM, 22(11):612–613, 1979.
64. B. Skoric and P. Tuyls. Secret key generation from classical physics. *Philips Research Book Series*, September 2005.
65. K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. *IEEE Micro*, 21(6):43–49, 2001.
66. G. Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy, March 2006. IEEE Press.
67. P. Tuyls and L. Batina. RFID-tags for anti-counterfeiting. In *Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006*, Lecture Notes in Computer Science, San Jose, California, USA, February 2006. Springer.
68. I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *Second Workshop on Security in Ubiquitous Computing*, Seattle, WA, USA, 2003.
69. S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *International Conference on Security in Pervasive Computing*, LNCS, 2802, pages 454–469, Germany, March 2004. Springer.
70. D. Wheeler and R. Needham. TEA, a Tiny Encryption Algorithm. In *Fast Software Encryption: Second International Workshop, Leuven, Belgium, December*, volume 1008 of *Lecture Notes in Computer Science*, pages 363–366. Springer, 1995.
71. S. Wolfram. *A new kind of science*. Wolfram Media Inc., Champaign, USA, 2002.
72. J. Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.